REMARKS

This communication is in response to the Final Office Action mailed July 12, 2004 in connection with the above-identified matter. Claims 14-26 remain pending in this application with claims 14 and 19 being the only independent claims. Reconsideration of the outstanding rejections in view of the amendments to the claims and remarks presented below is respectfully requested.

On a formal note, the Examiner has provided with the outstanding Office Action an initialed PTO Form 1449 of the references submitted with the Information Disclosure Statement filed simultaneously with the application. Six foreign references were identified on the PTO Form 1449, of which a full translation was not provided for two of the six references, namely, DE 195 27 715 and EP 0 481 714. The Examiner failed to initial these two references as having been considered yet never mentioned any reasoning in the Office Action itself for doing so. In the Information Disclosure Statement submitted with the application, as originally filed, applicant satisfied the concise statement of the relevancy of these foreign patents with the text which has been reproduced below for the Examiner's convenience.

"All but one reference listed in the accompanying PTO Form 1449 were identified in an International Search Report in the PCT application to which the present U.S. National Phase patent application claims priority. A copy of the search report is provided. For those reference listed on the PTO Form 1449 which are in a foreign language, however, the requirements pursuant to 37 CFR 1.96 for a concise explanation of the relevancy of each foreign reference have been satisfied. In particular, the search report satisfies the concise explanation requirement in that it provides the degree of relevance of each non-English reference.

One reference, the DE 195 27 715 was uncovered by the German Patent Office. The reference was characterized as pertinent only to the preamble of claim 1 of the German claims."

Applicant submits that the statements provided in the Information Disclosure Statement that accompanied the PTO Form 1449 satisfy the requirements associated with providing a concise explanation of the relevancy of each foreign reference. Accordingly, applicant requests that the Examiner in the next communication provide a copy of the PTO Form 1449 will all six references initialed as having been considered.

Applicant respectfully traverses the finality of the outstanding Office Action. MPEP section 706.07(a) states "Under present practice, second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is neither necessitated by applicant's amendment of the claims nor based on information submitted in an information disclosure statement filed during the period set forth in 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p)." Addressing the second situation, the only Information Disclosure Statement in connection with this matter was submitted simultaneously with the application, thus this second situation is not applicable. Accordingly, the only permissible way the outstanding Office Action could be made final and still introduce a new ground of rejection is if, and only if, the new ground of rejection is necessitated by applicant's amendment of the claims.

In the Amendment filed on April 14, 2004, applicant amended the claims to correct for grammatical errors and to conform with customary U.S. patent drafting rules, not to overcome the prior art rejections. Specifically, the preamble of independent claims 14 and 19 were amended to correct for grammatical errors that occurred through translation. The phrase "wherein at the manufacturer for pre-personalizing the chip" was found in the preamble of the claim, as originally filed, but in a different location. Applicant deleted the "optionally" indefinite language from the preamble and thus repositioned some of the other existing text in the preamble. No substantive changes were made to the preamble. The amendments to the limitations in the body of claims 14 and 19 as well as those amendments to the dependent claims and new claims added are merely technical in nature to restate, for clarification, the true text that each acronym represents, to correct for improper antecedent basis of a term, to insert the acronym associated with its corresponding phrase, to correct for a typographical error, or to delete indefinite subject matter to be recited instead in a dependent claim. Once again such

amendments do not invoke substantive changes that would necessitate a new grounds for prior art rejection. Accordingly, since the new grounds of prior art rejection are not necessitated by the April 14, 2004 amendment, applicant submits that the finality of the outstanding Office Action is premature and requests that it be withdrawn.

On a formal note, the Examiner stated in the fourth paragraph of the outstanding Office Action that the amendment to the claims filed on April 14, 2004 fails to comply with the requirements of 37 CFR 1.121(c) because the amended claims contain various words and lettering inside double brackets, which makes the claims confusing. In particular, the Examiner refers to in claim 14, the third line that reads "[[and]] a card number", and in lines 12-12 "[[a]] the secret key [[K1]] Ki". Applicant draws the Examiner's attention to section (c)(2) of 37 CFR 1.121 which the Examiner reproduced in its entirety in the outstanding Office Action. Specifically, the relevant sentence in that particular section (as found on page 3 of the outstanding Office Action) states "The test of any deleted matter must be shown by strike-through *except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived.")(italics added).* The relevant claim text cited by the Examiner as being bounded on either side by double italics denotes subject matter of five or fewer consecutive characters to be deleted, as permitted by the rules. Withdrawal of the Examiner's objection is therefore requested.

Claims 19-22 and 26 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,883,960 (the '960 patent). Claims 14, 15, 23, 24 and 25 are rejected under 35 U.S.C. §103(a) as obvious over the '960 patent in view of U.S. Patent No. 5,557,679 (the '679 patent). Claims 16-18 are rejected under 35 U.S.C. §103(a) as obvious over the '960 patent and the '679 patent in view of U.S. Patent No. 5,793,866 (the '866 patent).

Independent claim 19 is rejected as anticipated by the '960 patent. The Examiner in the outstanding Office Action states that the '960 patent reads on the limitation "wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki are stored" as disclosed in Col. 9, ll. 21-29.

Indeed, the relevant passage of the '960 patent teaches that a secret key KD_{COB} of the chip on board (COB) 22 is written into its associated ROM 34, however, the reference is silent concerning the storing of "a subscriber identification number (IMSI)" and "a card number (ICCID)", as expressly claimed.

Furthermore, the next limitation addressed by the Examiner with respect to independent claim 19 provides "wherein the chip itself derives an initial secret key Ki_1" which the Examiner states is taught by Col. 14, ll. 42-55. The passage in question of the '960 patent is reproduced below for convenience.

> "Referring next to FIG.8, the controller of the mobile unit sends a telephone number request message, containing the above-data, to the carrier's terminal (step m). The carrier's terminal performs decryption using the carrier secret key KD_{CN}, obtains KE_{MSNm}, and checks if the decrypted KE_{MSNm} matches any one of the previously registered KE_{MSNi}. If there is no match, the registration is denied. If there is a match, the credit card No. and the additional service information are recovered using the KE_{MSNm}. The recovered credit card No. is reported to the credit company's database 80 via the public network 82 (FIG. 5) for automatic investigation of the applicant's credit; if the result is OK, an assigned telephone number (DN) is received from the customer management system (step n). The telephone number received from the customer management system is encrypted with the mobile unit public key KE_{MSNm} and transferred to the controller of the mobile unit (step o). Upon receiving the encrypted telephone number $E(KE_{MSNm}, DN)$, the controller of the mobile unit sends the command of item No. 12, containing the encrypted telephone number and the mobile unit secret key KD_{MSNm}, to the internal COB for encrypt calculation (step p), and then, receives the result of the calculations, i.e., the telephone number, which is displayed (step q)."

It is the secret key KD_{COB} that is stored by the manufacturer in the COB during manufacture (Col. 8, ll. 21-29). Accordingly, in order to anticipate the claimed limitation, the '960 patent would have to disclose that "the *chip itself* derives an initial secret key Ki_1" from the chip secret key KD_{COB} stored in chip by the manufacturer (emphasis added). The passage of text above cited from the '960 patent fails to discuss any secret key associated with the COB (i.e., the chip itself) instead focusing only those secret keys associated with the mobile unit, e.g., KD_{MSNm}. Nor does the passage in question state that the secret keys associated with the mobile unit are in any way derived from the secret key associated with the COB. To the contrary, the

'960 patent discloses (Col. 8, ll. 40, 41) that "the mobile unit secret key KD_{MSNi} is known only to the manufacture of the mobile unit, and thus is not derived from the chip (COB) itself, as expressly found in claim 19.

Lastly, the Examiner asserts that the '960 patent teaches in Col. 14, l. 63 – Col. 15, l. 9, the limitation "wherein the chip in the terminal equipment is Toolkit-enabled and includes means for communication with a security center (SC) and negotiating a new secret key Ki_2." The relevant passage of the '960 patent is produced below.

> "Then, the personal information is signature encrypted with the carrier secret key KD_{CN}, and is further encrypted with the mobile unit public key KE_{MSNm} to produce $E(KE_{MSNm}, E(KD_{CN}, ID))$, which is then transmitted from the carrier's terminal to the controller of the mobile unit along with $E(KD_{CN}, KE_{MSNm})$ which is the mobile unit public key KD_{MSNm} signature-encrypted with the carrier secret key KD_{CN} (step t). The controller of the mobile unit enters the command of item No. 6, containing the received $E(KD_{CN}, KE_{MSNm})$, into the internal COB, thus writing KE_{MSNm} (step u), and then enters the command of item No. 8, containing the received $E(KE_{MSNm}, E(KD_{CN}, ID))$ and the $E(KD_{CN}, RDM)$ previously received in step g, into the internal COB, thus writing the personal information (step v)."

The passage quoted above from the '960 patent fails to disclose the chip (i.e., the COB) being Toolkit-enabled, nor that the chip (e.g., COB) has a component for communicating with a security center much less means included in the chip for negotiating a new secret key. Once again, the passage fails to discuss the secret keys associated with the chip (e.g., KD_{COB}) instead focusing only on the secret key of the mobility unit (e.g., KD_{MSNm}) and of the carrier (KD_{CN}), neither which are negotiated by components in the chip (e.g. COB), as expressly claimed.

The other independent claim, that is claim 14, is rejected as obvious over the '960 patent in view of the '679 patent. Addressing separately each limitation of claim 14, as parsed by the Examiner. Claim 14 states in the preamble "A method for personalizing GSM chips" to which the Examiner refers to Col. 4, ll. 6-9 of the '960 patent as teaching this limitation. The relevant passage referred to by the Examiner discloses a communication system but fails to disclose or suggest specifically a GMS (Global System Mobile) communication system as the cellular system.

Still addressing the preamble, the next limitation states, "wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki are stored". This passage is patentable over the prior art reference for the same reasons provide above with respect to independent claim 19 wherein the Examiner referred to the same passage of the prior art reference for teaching the claimed limitation.

Limitation b) in the body of claim 14 states "obtaining the (ICCID) card number and the (IMSI) subscriber identification number from a number pool, the chip itself derives an initial secret key Ki_1 from the secret key Ki which is known and entered into the chip". Applicant for the reasons stated above has distinguished with respect to claim 19 why the '960 patent fails to teach "the chip itself derives an initial secret key Ki_1 from the secret key Ki which is known and entered into the chip". Therefore, limitation b) of claim 14 having similar language is patentable over the art of record for the same reasons.

The next four limitations, limitations c)-f), states "c) making an entry in an authentication center (ACF) and a home location register (HLR) as soon as the subscriber has entered into a contract with a network operator; d) deriving at the authentication center (AC) the initial secret key Ki_1; e) setting the conditions of the network so that during logon to the network a connection is established from the chip to the security center (SC) of the network operator; f) routing the connection from the chip to the security center (SC) during the first logon". These limitations have been lumped together by the Examiner. The relevant passage cited by the Examiner is Col. 21, l. 19 – Col. 22, l. 7 of the '960 patent that states:

> "Upon receiving the random number RDM, the IC card registration terminal stores the same into its RAM, and at the same time, sends a registration start request message, containing the random number RDM, to the carrier's terminal (step d). Upon receiving the random number RDM, the carrier's terminal signature encrypts the received random number RDM with the carrier secret key KD_{CN}, and returns the result $E(KD_{CN}, RDM)$ (step e). Upon receiving $E(KD_{CN}, RDM)$ the IC card registration terminal sends the command of item No. 11 in Table 2 containing the received $E(KD_{CN}, RDM)$, the RDM stored in its RAM and the integer I (I=1) to the internal COB (step f) to read out the carrier public key KE_{CN} (step g). Next, a message is displayed on the display prompting the operator to input the dealer number when the dealer number is entered (step h). the command of item No. 12 in Table 2 is entered twice to request the internal COB for encrypt calculation (step i), as a result of which $E(KE_{CN}, KE_{AN})$, the

registration terminal public key KE_{AN} encrypted with the carrier public key KE_{CN}, and E(KE_{CN}, dealer number), the dealer number encrypted with KE_{CN}, are received (step j).

Referring next to Fig. 30, the registration terminal sends a registration request message, containing the above data, to the carrier's terminal (step k). The carrier's terminal decrypts the data using the carrier secret key KD_{CN}, to derive the dealer's number and KE_{CN} which are then compared with the dealer numbers and KE_{AN} is stored in the carrier's terminal for a match (step i). If a match is found E(KD_{CN}, KE_{AN}), KE_{AN} signature-encrypted with KD_{CN} and E(KE_{AN}, e(KD_{CN}, ID_{AN})), the registration terminal ID assigned to the registration terminal signature-encrypted with KD_{CN} with the result further encrypted with KE_{AN}, are sent back (step m). Upon receiving these data, the registration terminal writes KE_{AN} into the internal COB device by using the command of item No. 6 (step n), and ID_{AN} into the same by using the command of item No. 8 (step o)."

The passage above cited by the Examiner discusses the registration sequence associated with the IC card registration. This passage fails to disclose an authentication center, security center or a home location register, much less the specific limitations concerning the authentication center, security center and/or home location register as found in limitations c)-f).

Limitation g) states "negotiating between the chip and the security center (SC) a new second secret key Ki_2". The Examiner rejects this limitation as being obvious over Col. 14., l. 63 – Col. 15, l. 9 of the '960 patent which has been reproduced above. The passage in question fails to disclose or suggest a security center, much less, that the chip (e.g., COB) and security center negotiate a new second secret key Ki_2, as claimed.

With respect to the last limitation of claim 14 the Examiner states "disabling the conditions of step e)" is taught by Col. 14, ll. 3-14 of the '960 patent. To reiterate, the conditions set forth in step e) that are to be disabled are "setting the conditions of the network so that during logon to the network a connection is established from the chip to the security center (SC) of the network operator". The reason for disabling in step g) the conditions of step e) is that this operation need only be performed once. In contrast, the relevant passage of the '960 patent cited by the Examiner states:

"If they do not match the readout result NG is returned. Upon receiving the readout result NG, the controller of the mobile unit updates the value of I to I+1 and again sends the command of item No. 11 to the internal COB (step b). If KE_{CN} cannot be read out even when the value of I has reached a predetermined

value, this means that the KE_{CN} for the communications network to which the applicant desires to subscribe is not stored in the COD in the mobile unit, i.e., it is found that the mobile unit that requested registration cannot be used in the communications network to which the applicant desires to subscribe."

Claim 14 is distinguishable over the passage cited by the Examiner in several respects. First, unlike the present claimed invention in which disabling of the conditions of step e) is not conditional but occurs every time, the relevant text of the '960 patent text teaches that if a condition occurs, e.g., the value I reaches a predetermined value, a classification is made that the communications network to which the applicant desires to subscribe is not stored in the COD in the mobile unit. No disabling is mentioned, much less those specifically enumerated in step e) of the present claimed invention.

Dependent claims 15, 20, 21, 24 and 26 are further distinguishable over the '960 patent in that each involves communication with a security center. Specifically, claim 15 states "wherein the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the authentication center (AC) before the contract is established"; claim 20 states "wherein the chip includes means for receiving date from the security center (SC) and means for writing the received data to the memory"; claim 21 states "wherein the chip comprises a microprocessor for negotiating a secret key with the security center (SC)"; claim 24 states "wherein step g) further comprises negotiating at the security center (SC) the PUK with the chip or generated in the security center (SC) and transmitted to the chip"; claim 26 states "wherein the chip includes means for reading data received from the security center (SC) in memory, modifying the data and transmitting the data to the security center (SC)". The '960 patent fails to mention a "security center" and/or "authentication center" whatsoever, much less, the specific limitations recited in the claims in question.

For the foregoing reasons applicant submits that independent claims 14 and 19 are patentable over the prior art of record. The remaining claims depend from one of these independent claims and thus are also patentable over the art of record. Applicant submits that the application is in condition for allowance and passage to issuance is respectfully requested.

If any additional fees are required, authorization is hereby provided to charge our U.S. Patent and Trademark Deposit Account No. 14-1263.

Respectfully submitted,

Christa Hildebrand

Christa Hildebrand
Reg. No. 34,953
Attorney for Applicant

Norris McLaughlin & Marcus P.C.
875 Third Avenue, 18th Floor
New York, N.Y. 10017
Telephone: (212)808-0700
Facsimile: (212)808-0844